ISSUES IN DEFENCE SCIENCE & TECHNOLOGY

ISSUE 6 **SEPTEMBER 1998**

The Defence Research and Development (R&D) Branch publishes *Issues in Defence Science and Technology* on an ad hoc basis with the aim of introducing significant and emerging defence S & T issues to senior officers and managers of the Canadian Forces and of the Department of National Defence. This publication is also available on the Defence Information Network (DIN).

Information Operations

THE ISSUE IN CONTEXT

"*The protection of one's own information capabilities and the exploitation of any potential adversary's information capabilities have become a fundamental principle of a nation's security*"[1].

How the information revolution affects the conduct of military operations and, more broadly, the security of the nation, is a critically important issue for the Department of National Defence (DND) and the Canadian Forces (CF).

The dependence of military institutions on technology-based information storage and retrieval systems has magnified the threat of "information warfare" (IW), i.e., overt and covert attacks against these systems and the information contained in them.[2] At the same time, other institutions responsible for critical information infrastructure services (such as the public telephone network) upon which the nation's economic security depend, are also increasingly vulnerable.[2]

Moreover, because the defence and civil information infrastructures are deeply intertwined, appropriate responses to the threat can only be arrived at by a coordinated approach involving government departments and agencies, as well as the commercial sector.

For DND and the CF, however, the scope of IW is not limited to conducting or defending against electronic attacks on computers and related information systems. It also encompasses the whole spectrum of possibilities for employing information effectively in conflict, and denying adversaries the same capability.

BACKGROUND

For Canadian purposes, IW has been subsumed into the larger concept of "Information Operations" (IO). As defined by the CF, IO mean actions taken in support of national objectives which influence decision-makers by affecting adversary information while exploiting and protecting one's own information. IO comprises two major subdivisions: Offensive and Defensive IO.[1]

Offensive IO includes actions taken to influence actual or potential adversarial decision-makers, and may be conducted by exploiting and affecting an adversary's use of or access to information and information systems.[1]

Offensive IO can include the application of psychological operations (PSYOPS), deception, Electronic Warfare (EW), intelligence, computer network attack, physical destruction, and Special Information Operations (SIO).[1]

Defensive IO includes actions taken to ensure friendly decision-makers have timely access to accurate information and are protected from any adversary Offensive IO efforts. Defensive IO strives to ensure the friendly decision-making process is protected from all adverse effects, either deliberate or inadvertent.

Defensive IO is a process that integrates and coordinates policies, procedures, operations, intelligence, law and technology.[1]

At the technology level, increasingly complex information systems are being integrated into traditional military operations such as transport, logistics; as well as command and control, communications; and intelligence.

The use of these information systems enhances all military operations, but these capabilities induce dependence, which in turn creates vulnerabilities.

These vulnerabilities are a double-edged sword, representing areas which must be protected, but also create new opportunities that can be exploited against adversaries. The R&D Branch is committed to contributing its unique S&T expertise to help the CF integrate systems, disciplines and techniques to achieve a coherent IO strategy that best employs this double-edged sword.

R&D BRANCH LEADERSHIP

To respond to the Information Operations Initiative, the R&D Branch is defining and initiating an R&D program in IO.

There are a number of areas in which common needs are recognized and agreed upon, and where opportunities for enhancing CF capabilities are seen. Related to computer networks and command and control systems, there are requirements for tools and tool-sets for network analysis, protection, intrusion detection, deception, reaction and engagement.

In its preliminary response, the R&D Branch has begun several new activities in Information

Protection. Together with the new Network Vulnerability Assessment Team (NVAT), a framework for assessment tools, called IRONMAN, is being developed.

Work has also begun on methods for detection of attacks on networks and Command, Control Information Systems (CCIS) IO safeguards. The vulnerability of networks must be understood and test-beds are required for the development of protection and engagement techniques.

In the broader IO domain, requirements in the electronic warfare area include, for example, fingerprinting communications signals, smart jamming against cellular networks, and determining the implications of threats against GPS navigation systems.

Protection is also required against the threat of high-power microwave and non-nuclear electromagnetic pulse attacks. Human factors also need to be examined to understand the interaction between users and information systems in an IO environment.

To fully address DND and CF needs, however, it will be necessary to develop within the Branch a core competency in Information Operations, particularly as it relates to Command & Control (C2) warfare and the ability to assess the strengths and weaknesses of distributed Information Technology (IT) systems.

At present, there are isolated pockets of expertise in certain areas, but Branch efforts are not yet as cohesive or comprehensive, as they must be to adequately address the issue. The Branch will also need to augment the effort with people possessing the appropriate skill sets.

Given Canada's competitive edge in information technology, Branch efforts on IO will benefit from an orchestrated development agreement with the private sector.[2] Indeed, the Defence Science Advisory Board (DSAB) has recommended that the Department encourage and fund the Branch to "...set up effective and focused partnerships with Industry in order to marshal scarce resources into collaborative efforts in the face of a common threat."[2]

CONCLUSIONS

The threat of IO affects both military and civilian infrastructure, indeed, the threat to civilian infrastructure may be the more serious national security issue. Branch efforts aim to address these threats and support the broader interests of the Federal Government.

Work already underway includes the development of a framework for network vulnerability assessment, called IRONMAN, and development of methods for detection of attacks on networks.

The Branch's response to the challenge of IO also includes efforts by the IO R&D Team to define a program of work that will satisfy the broader requirements of the CF to conduct offensive and defensive IO in support of national objectives.

To ensure DND and the Branch can adequately address the emerging challenges posed by IO, the DSAB has recommended "an enhanced level of resources" as well as the establishment, by the Branch, of broad development agreements with the private sector as a means of leveraging resources to meet these challenges.

In cooperation with our partners in DND and in other government departments, the Branch is actively planning this enhanced program.

For more information on the Branch *Information Operations* initiatives, please contact Gordon Marwood, Chief Scientist, DREO; ph: (613) 998-2237; e-mail: Gordon.Marwood@dreo.dnd.ca; or Dr. Malcolm Vant, Deputy Scientific Advisor (Command and Control Information Systems); ph: (613) 992-6601; e-mail: Malcolm.Vant@crad.dnd.ca

An excellent comprehensive analysis of Information Operations can be found in *"In Athena's Camp: Preparing for Conflict in the Information Age"* edited by John Arquilla & David Ronfeldt. RAND Corporation, 1997. The document can be found online in Adobe Acrobat format (.pdf) at this RAND corporation URL: http://www.rand.org/publications/MR/MR880/

Another RAND publication describing the impact of the information revolution on security issues is *"Strategic Information Warfare: A New Face of War"* by Molander et al. RAND Corporation, 1996. Available in Adobe Acrobat (.pdf) format at this RAND corporation URL: http://www.rand.org/publications/MR/MR661/MR661.pdf

1. CF Information Operations B-GG-005-004/AF-033. April 1998.
2. DSAB Report 97/1. Information Operations. March 1998.

(Return to Publications)

R&D Home | Search | Help | Français | Comments | D-NET Home

© Minister of Public Works and Government Services Canada

National Defence Défense nationale

Canada

QUESTIONS DE SCIENCES ET TECHNOLOGIE APPLIQUÉES À LA DÉFENSE

NUMÉRO 6 **SEPTEMBRE 1998**

La Direction recherche et developpement pour la Défense publie *Questions de science et technologie appliquées à la Défense* de façon ponctuelle afin de présenter aux officiers supérieurs et aux cadres des Forces Canadiennes et du ministère de la Défense nationale un aperçu des questions importantes et émergentes en matière de sciences et technologie liées à la défense. Ce document est également disponible sur le Réseau d'information de la défense (RID).

Opérations d'information

MISE EN SITUATION

« *La protection de ses propres moyens d'information et l'exploitation des moyens d'information de tout adversaire éventuel figurent désormais au nombre des principes fondamentaux de la sécurité des États* ».[1]

L'effet de la révolution de l'information sur la conduite des opérations militaires et sur la sécurité du pays en général est une question qui revêt une importance cruciale pour le ministère de la Défense nationale (MDN) et les Forces canadiennes (FC).

La dépendance des institutions militaires à l'égard des systèmes de stockage et d'extraction d'information reposant sur la technologie est venue amplifier la menace que constitue la « guerre de renseignement », c'est-à-dire les attaques ouvertes ou secrètes contre ces systèmes et l'information qu'ils renferment.[2] Parallèlement, d'autres institutions responsables de services d'infrastructures d'information critiques (tel le réseau téléphonique public), dont dépend la sécurité économique du pays, sont également de plus en plus vulnérables.[2] En outre, comme les infrastructures d'information militaires et civiles ont de forts liens entre elles, seule une approche concertée impliquant les ministères et organismes gouvernementaux et le secteur privé peut permettre de trouver des moyens appropriés de contrer cette menace.

Pour le MDN et les FC, toutefois, la « guerre de renseignement » ne se limite pas à mener ou à contrer des attaques électroniques au moyen d'ordinateurs et de systèmes d'information connexes. Elle couvre également tout le spectre des possibilités d'utilisation efficace de l'information lors d'un conflit, tout en empêchant l'ennemi d'avoir accès à ces mêmes moyens.

CONTEXTE

Pour les besoins de la situation proprement canadienne, la « guerre de renseignement » a été incorporée au concept plus large des « opérations d'information » (OI). Selon le sens que leur donnent les Forces canadiennes, les OI désignent les mesures prises à l'appui d'objectifs nationaux, qui influencent les décideurs en affectant l'information adverse tout en exploitant et en protégeant sa propre information. Les OI se divisent en OI offensives et OI défensives.[1]

Les OI offensives comprennent les mesures prises afin d'influencer les décideurs adverses réels ou potentiels. Elles consistent à exploiter l'information et les systèmes d'information de l'adversaire ainsi qu'à nuire à sa capacité d'utiliser cette information ou ces systèmes ou d'y avoir accès1. Au nombre des OI offensives, il convient de mentionner les opérations psychologiques, les leurres, la guerre électronique, le renseignement, l'attaque des réseaux d'ordinateurs, la destruction physique et les opérations d'information spéciales (OIS).[1]

Les OI défensives concernent les mesures prises afin d'avoir l'assurance que les décideurs amis ont rapidement accès à de l'information exacte et sont protégés contre toute OI offensive menée par l'adversaire. Les OI défensives visent à faire en sorte que le processus décisionnel ami soit protégé contre tout effet préjudiciable, qu'il soit délibéré ou non. Les OI défensives constituent un processus qui regroupe et coordonne des politiques, des procédures, des opérations, les activités de renseignement, les lois et la technologie.[1]

En ce qui concerne la technologie, des systèmes d'information de plus en plus complexes sont intégrés aux opérations militaires traditionnelles, telles que les transports et la logistique, le commandement et le contrôle, les communications et le renseignement. L'utilisation de ces systèmes d'information améliore les opérations militaires, mais ces moyens entraînent une dépendance, qui, à son tour, suscite des vulnérabilités.

Ces vulnérabilités constituent une arme à deux tranchants en ce sens qu'elles représentent des domaines à protéger impérativement, mais créent également des possibilités pouvant être exploitées contre les adversaires. La Direction R et D s'est engagée à mettre ses compétences scientifiques et techniques à contribution afin d'aider les FC à intégrer les systèmes, les disciplines et les techniques nécessaires à la mise en place, en matière d'OI, d'une stratégie cohérente qui tire le meilleur parti possible de cette arme à deux tranchants.

CONTRIBUTION DE LA DIRECTION DE LA R ET D

Pour donner suite à l'initiative concernant les opérations d'information, la Direction R et D a entrepris de définir et de lancer un programme de R et D consacré à ces opérations.

Il existe un certain nombre de secteurs où des besoins communs ont été constatés et font l'objet d'un consensus; ce sont également des secteurs où il apparaît possible d'améliorer les capacités des FC. Par rapport aux réseaux d'ordinateurs et aux systèmes de commandement et de contrôle, il s'avère nécessaire d'élaborer des outils d'analyse de réseaux, de protection, de détection des intrusions, de déception, de réaction et d'engagement.

Comme intervention préliminaire, la Direction R et D a lancé plusieurs activités nouvelles dans le

domaine de la protection de l'information. La formation de la nouvelle équipe d'évaluation de la vulnérabilité des réseaux s'accompagne de la mise en place d'un cadre d'élaboration d'outils d'évaluation baptisé IRONMAN. On a également amorcé l'établissement de méthodes de détection des attaques contre les réseaux et de mesures de sauvegarde des opérations d'information des Systèmes d'information de commandement et de contrôle. Il importe de bien saisir la vulnérabilité des réseaux et de mettre au point des bancs d'essai en vue de l'élaboration de techniques de protection et d'engagement.

Dans le domaine plus large des opérations d'information, la guerre électronique exige notamment l'identification des signaux de communication, le brouillage intelligent contre les réseaux cellulaires et la détermination de l'incidence des menaces contre les systèmes de navigation GPS. Il importe également d'assurer une protection contre la menace que représentent les armes hyperfréquences de haute puissance et les armes à impulsion électromagnétique non nucléaires. Enfin, il convient d'examiner les facteurs humains afin de comprendre l'interaction des utilisateurs et des systèmes d'information dans les OI.

Pour satisfaire pleinement aux besoins du MDN et des FC, toutefois, il faudra doter la Direction d'un noyau de compétences en opérations d'information, notamment en ce qui concerne la guerre C2 (Commandement et contrôle) et la capacité d'évaluer les forces et les faiblesses des systèmes de technologie de l'information répartis. À l'heure actuelle, il existe des compétences isolées dans certains domaines, mais les efforts de la Direction ne sont pas encore aussi cohérents ou complets qu'ils devraient l'être. La Direction devra aussi accroître son effort en se dotant d'effectifs possédant les combinaisons de compétences appropriées. Étant donné l'avantage concurrentiel que possède le Canada dans le domaine de la technologie de l'information, la Direction pourra tirer profit de la conclusion d'un accord de concertation avec le secteur privé2. En fait, le Conseil consultatif sur les sciences appliquées à la défense a recommandé que le Ministère fournisse à la Direction l'incitation et les crédits nécessaires à la formation de partenariats efficaces et focalisés avec le secteur privé, afin de mobiliser les ressources limitées et de susciter des collaborations face à une menace commune.[2]

CONCLUSIONS

La menace liée aux OI concerne à la fois l'infrastructure militaire et l'infrastructure civile. En fait, la menace qui pèse sur l'infrastructure civile est peut-être plus grave du point de vue de la sécurité nationale. Les efforts de la Direction visent à contrer ces menaces et à défendre l'intérêt supérieur du gouvernement fédéral.

Parmi les travaux déjà en cours, il convient de mentionner l'élaboration d'un cadre d'évaluation de la vulnérabilité des réseaux, baptisé IRONMAN, et l'établissement de méthodes de détection des attaques contre les réseaux.

Pour relever le défi que représentent les OI, la Direction s'est dotée d'une équipe de R et D sur les OI ayant pour mandat de définir un programme de travail qui répondra aux besoins généraux des FC pour la conduite d'OI offensives et défensives destinées à soutenir les objectifs nationaux.

Pour que le MDN et la Direction puissent relever convenablement les défis nouveaux que représentent les OI, le Conseil consultatif sur les sciences appliquées à la défense a recommandé « un niveau de ressources amélioré » ainsi que la conclusion par la Direction d'accords généraux avec le secteur privé afin de réunir les ressources nécessaires pour relever ces nouveaux défis. La

Direction s'emploie activement à planifier ce programme amélioré, de concert avec nos partenaires du MDN et des autres ministères.

Pour obtenir des plus amples rensiegnements sur ce sujet veuillez communiquer avec M. Gordon Marwood, Scientifique principal, CRDO, tél: (613) 998-2237, adresse électronique: Gordon.Marwood@dreo.dnd.ca; ou le Dr. Malcolm Vant, Conseiller scientifique adjoint systémes d'information de commandment et de contrle (CSASICC), tél: (613) 992-6601; adresse électronique: Malcolm.Vant@crad.dnd.ca.

On trouvera une excellente et exhaustive analyse des opérations d'information dans le document intitulé *« In Athena's Camp: Preparing for Conflict in the Information Age »* édité par John Arquilla et David Ronfeldt. RAND Corporation, 1997. La version électronique de ce document est présentée en format Adobe Acrobat (.pdf) à l'adresse URL suivante de la corporation RAND : http://www.rand.org/publications/MR/MR880/

Une autre publication de la corporation RAND décrit l'effet de la révolution de l'information sur les questions de sécurité. Il s'agit du document intitulé *« Strategic Information Warfare: A New Face of War »* de Molander et coll. RAND Corporation, 1996. Disponible en format Adobe Acrobat (.pdf) à l'adresse URL suivante de la corporation RAND : http://www.rand.org/publications/MR/MR661/MR661.pdf

1. CF Information Operations B-GG-005-004/AF-033. Avril 1998.
2. Rapport 97/1 du CCSAD. Opérations d'information. Mars 1998

(Retour à Publications)

Menu R et D | Recherche | Aide | English | Commentaires | Menu D-NET

© Ministre des Travaux publics et Services gouvernementaux Canada

Défense nationale National Defence

Canada